Computer Networks

Dr. Ali Sayyed
Department of Computer Science
National University of Computer & Emerging Sciences

Network Security

What is security?

- Security prevent bad things from happening
  - Confidential information leaked
  - Important information damaged
  - Critical data / services unavailable
  - Critical data changed by unauthorized user
  - Data stolen
  - Improper access to resources
  - Data used to violate law
  - Data used for financial and personal gains

Network Security

- **Network security** measures are needed to protect data during the transmission and to guarantee that data transmissions are authentic.

Security Requirements

- To understand the types of threats to security that exist, we need to have a definition of security requirements. Network security address four requirements:
  - **Confidentiality**: Requires that data only be accessible by authorized parties.
  - **Integrity**: Requires that only authorized parties can modify data. Modification includes writing, changing, changing status, deleting, and creating.
  - **Availability**: Requires that data are available to authorized users.
  - **Authentication**: Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be.

Confidentiality with Symmetric Encryption

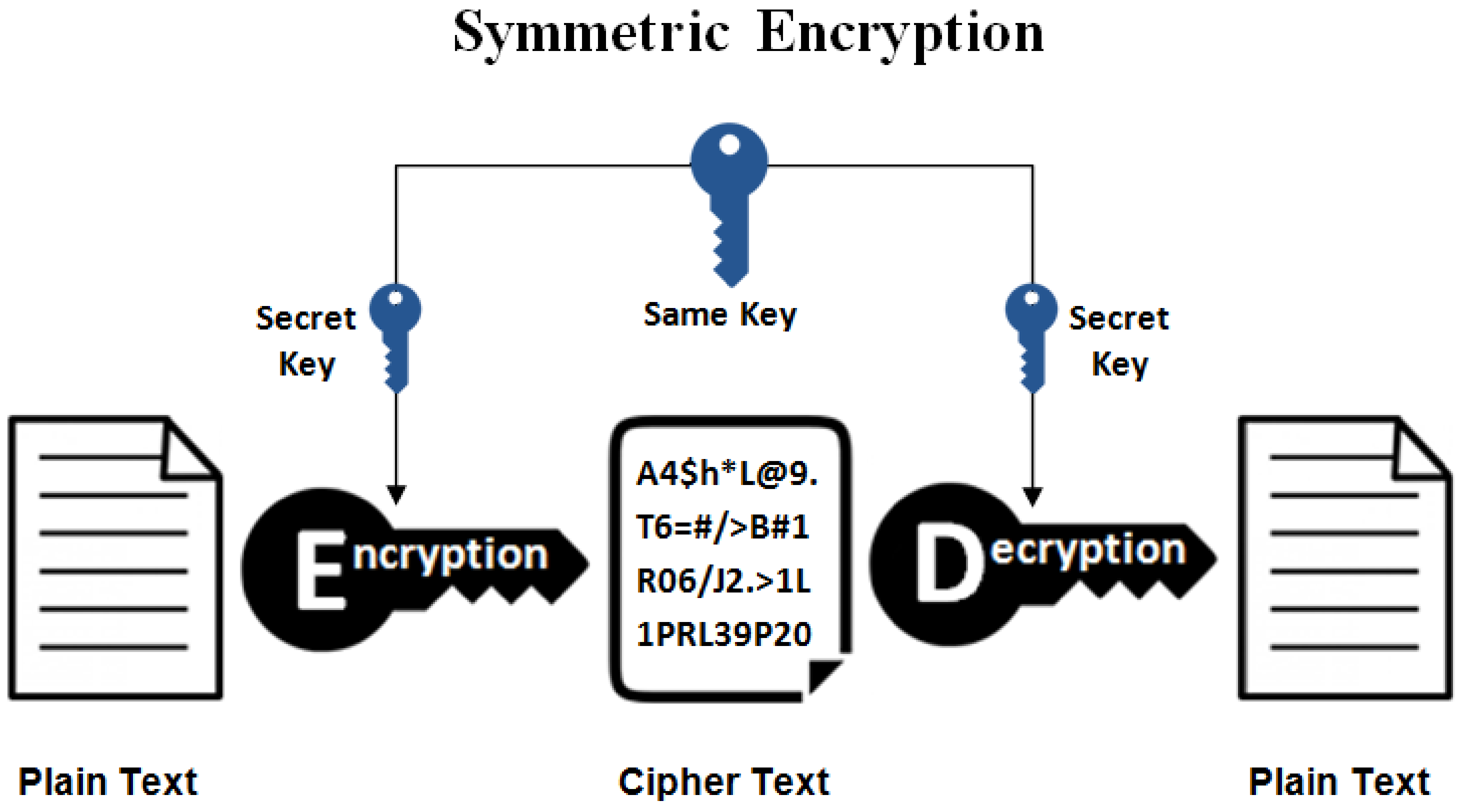
- Symmetric Encryption is the universal technique for providing confidentiality
- **What is Encryption:** An algorithm (program) encodes or scrambles information during transmission or storage. The information can be decoded/unscrambled by only authorized individuals.
- Simplest building blocks of encryption are:
  - **Substitution:** in which each letter/symbol is exchanged/replaced for another
  - **Transposition:** in which the order of letters/symbols is rearranged.
- It might seem that these are too simple to be effective. But almost all modern commercial symmetric ciphers use some combination of substitution and transposition for encryption.

Some Basic Encryption Terminology

- **Plain Text** - original message
- **Cipher Text** - coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher, known only to sender/receiver
- **Encipher** (encrypt) - converting plaintext to ciphertext
- **Decipher** (decrypt) - recovering plaintext from ciphertext

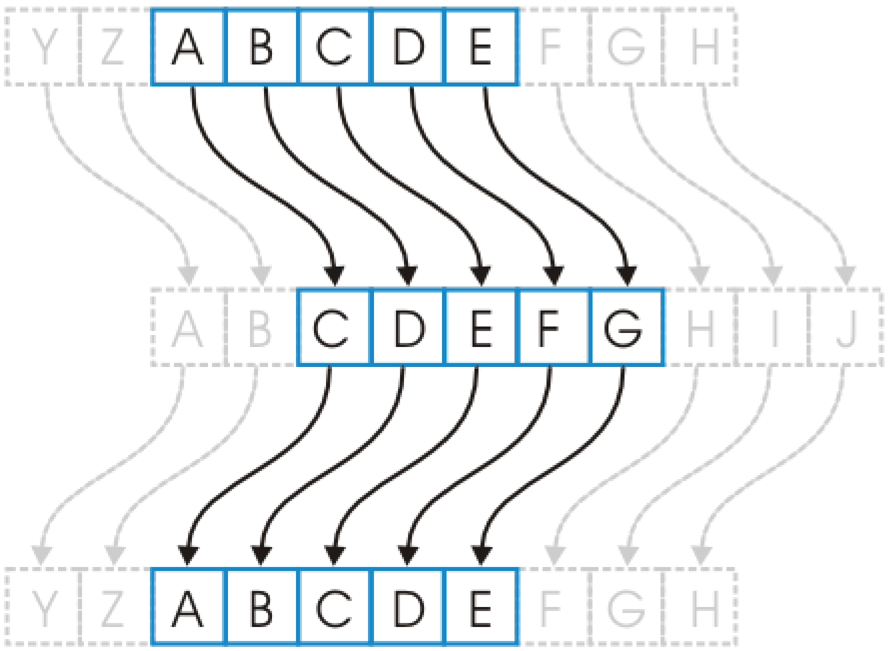
Confidentiality with Symmetric Encryption

- **Symmetric algorithms**: (also called "secret key" or Private Key) use the same key for both encryption and decryption;



Caesar Cipher

- By Julius Caesar
- earliest known **substitution cipher**
- core idea is to replace letter with another according to the Key
- Example:
  - **Plaintext**: meet me after the party
  - **Key** : 2
  - **Ciphertext**: oggv og chvgt vjg rctva
- Decryption should simply reverse the order according to the same key



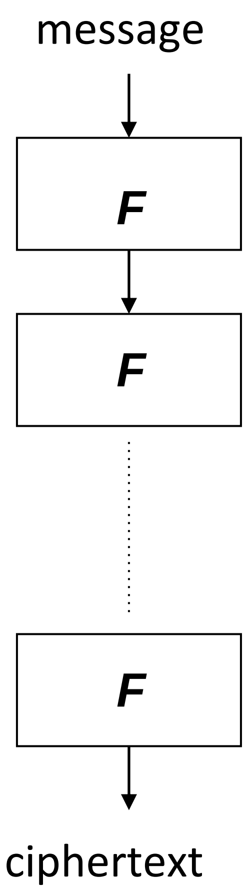
Columnar Transposition

- A **transposition Cipher**
- Arrange the plaintext into a matrix with columns equal to the key. Then take a transpose of the matrix.
- Add padding (random characters) to the end to make each column equal.
- Example
- **Plaintext**: WE ARE DISCOVERED FLEE AT ONCE
- **Key:** 6
- **Ciphertext**: WIREEES……

W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

Iterative cipher and Product cipher

- **Iterative Cipher**
  - An iterative cipher is one that encrypts a plaintext by repeatedly using the same technique using several rounds.
  - iterative F rounds until it is "secure"
- **Product Ciphers**
  - Product Ciphers consider several ciphers in succession
  - A substitution followed by a transposition makes a new much harder cipher
  - Rotor machine is an example



AES

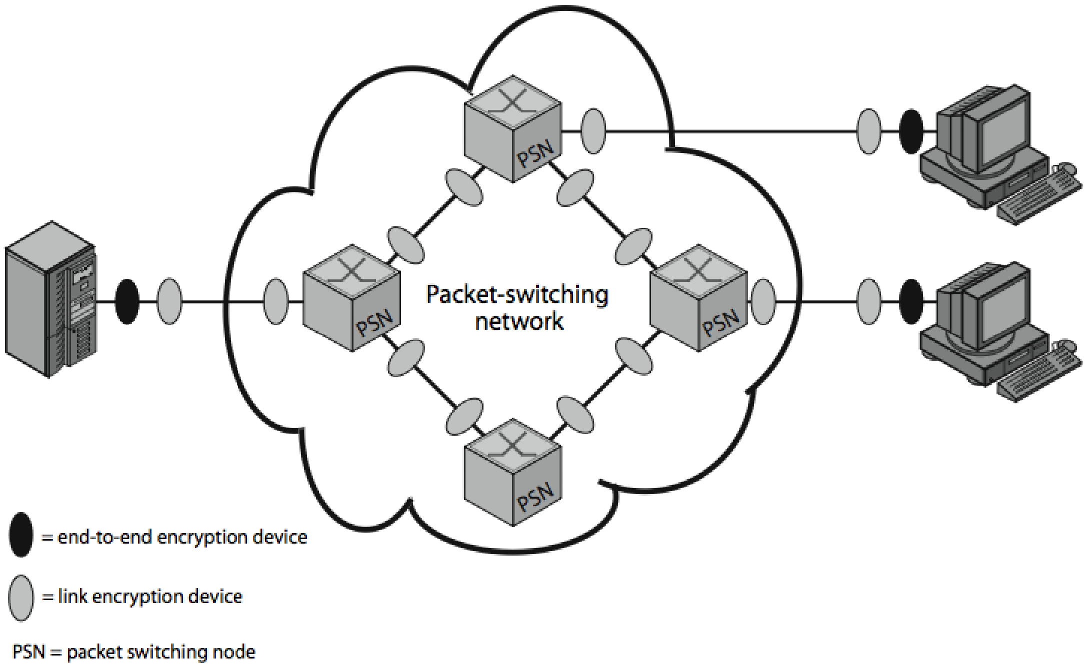
- AES (Advanced Encryption Standard) is a modern symmetric key cipher
- Both Iterative Cipher and Product Ciphers
- Used for the encryption of electronic data and operates on bits.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each
- AES (256 bit key)
  - Fifty supercomputers that could check a billion billion (10^{18}) AES keys per second (if such a device could ever be made) would, in theory, require about 3×10^{51} years to exhaust the 256-bit key space

Key Distribution

- Symmetric schemes require both parties to share a common secret key
- Issue is how to securely distribute this key
- This is one of the most critical areas in security systems.
- The strength of any cryptographic system depends on the key distribution technique.
- For two parties A and B key distribution can be achieved in a number of ways:
  - A can select key and physically deliver to B
  - if A & B have secure communications with a third party C, C can relay key between A & B

Placement of Encryption

- Symmetric encryption is used to provide message confidentiality
- have two major placement alternatives
- **Link encryption**
  - encryption occurs independently on every link
  - Traffic between links must be decrypted
  - requires many devices, and paired keys
- **end-to-end encryption**
  - encryption occurs between original source and final destination
  - need devices at each end with shared keys



Placement of Encryption

- With end-to-end encryption
  - User data is secure, but the traffic pattern is not
  - Because packet headers are transmitted without encryption, so that network can correctly route information
- Hence although contents are protected, traffic pattern are not
- Ideally want both at once
  - end-to-end protects data contents over entire path and provides authentication
  - link protects traffic flows from monitoring

Message Authentication

- A message, file, or document is said to be authentic when it is genuine and came from its alleged source.

- Message authentication is a procedure that allows communicating parties to verify that received messages are authentic.

- The two important aspects are to verify that the contents of the message have not been altered and that the source is authentic.

Authentication Using Symmetric Encryption

- It is possible to perform authentication simply by the use of symmetric encryption.
- If we assume that only the sender and receiver share a key, then only the genuine sender would be able successfully to encrypt a message for the other participant.
- But, is there any Problem
- Yes, Repudiation (to deny)
- Symmetric encryption cannot ensure **Nonrepudiation**.
- Typically, nonrepudiation refers to the ability to ensure that a party in a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Public-Key Cryptography

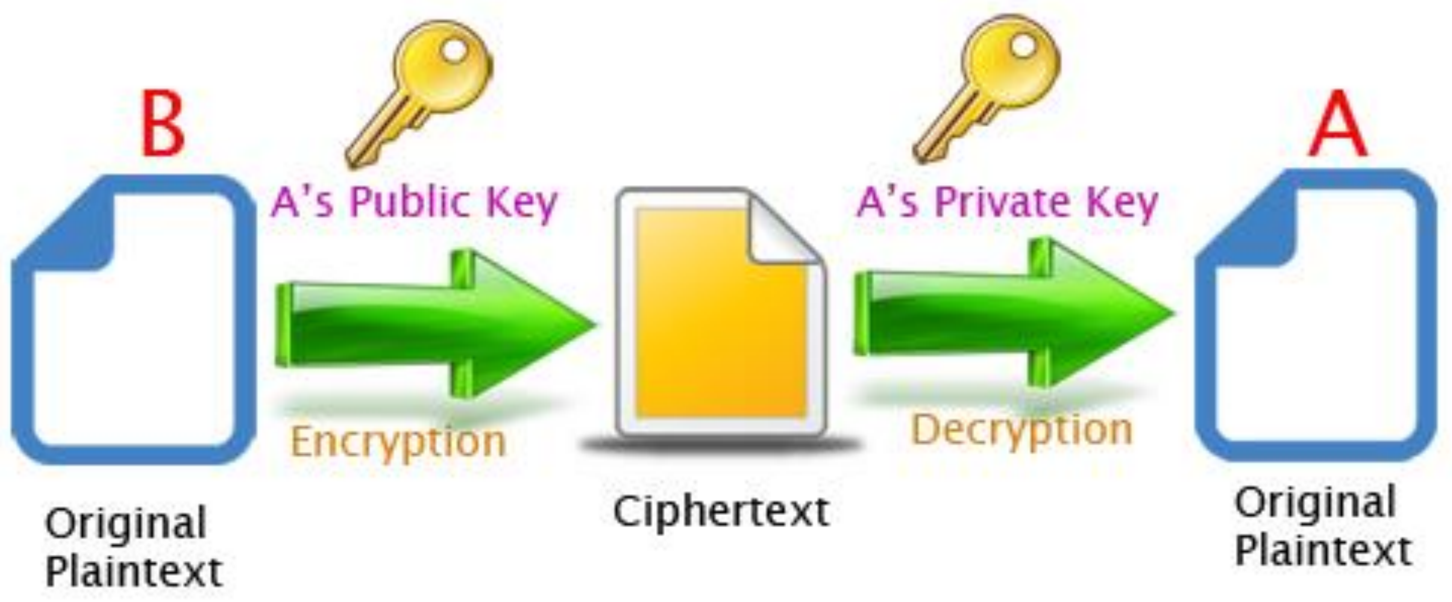
- Public-Key Cryptography uses two keys – a public & a private key
- asymmetric since parties are not equal
- uses clever application of numbers theory to function
- developed to address two key issues:
  - **Key distribution**
  - **Digital signatures (Authentication)**

Public-Key Encryption / Decryption

- Public-key encryption is a cryptographic system that uses two keys:
- A public key known to everyone and a private key known only to the Receiver.
- Public Key Locks (Encrypt)
- Private Key unlocks (Decrypt)

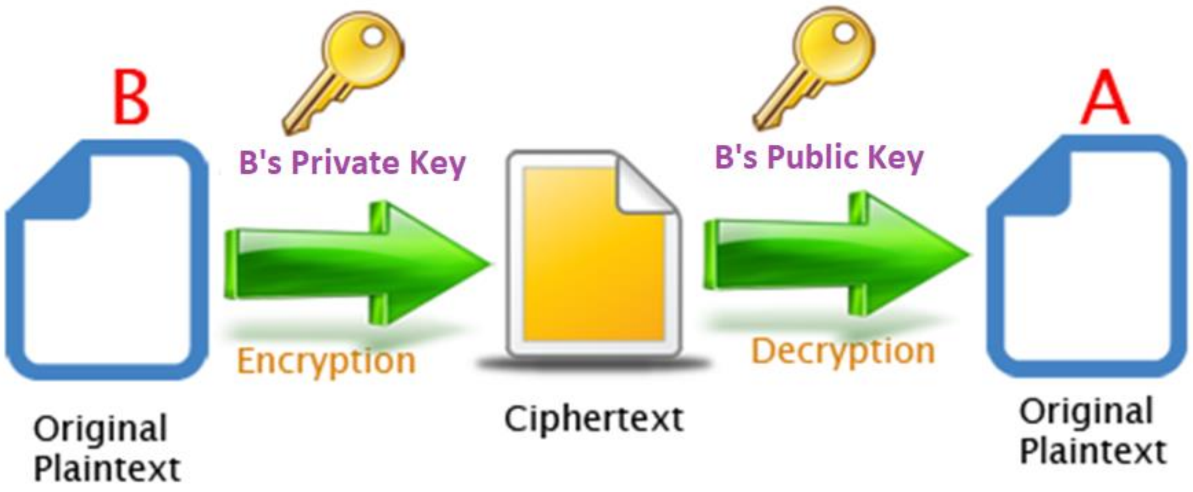
Public-Key Encryption / Decryption

- For Encryption, When B wants to send a secure message to A, B uses A's public key to encrypt the message.
- A then uses his private key to decrypt it.
- No need to distribute the Key



Digital signatures

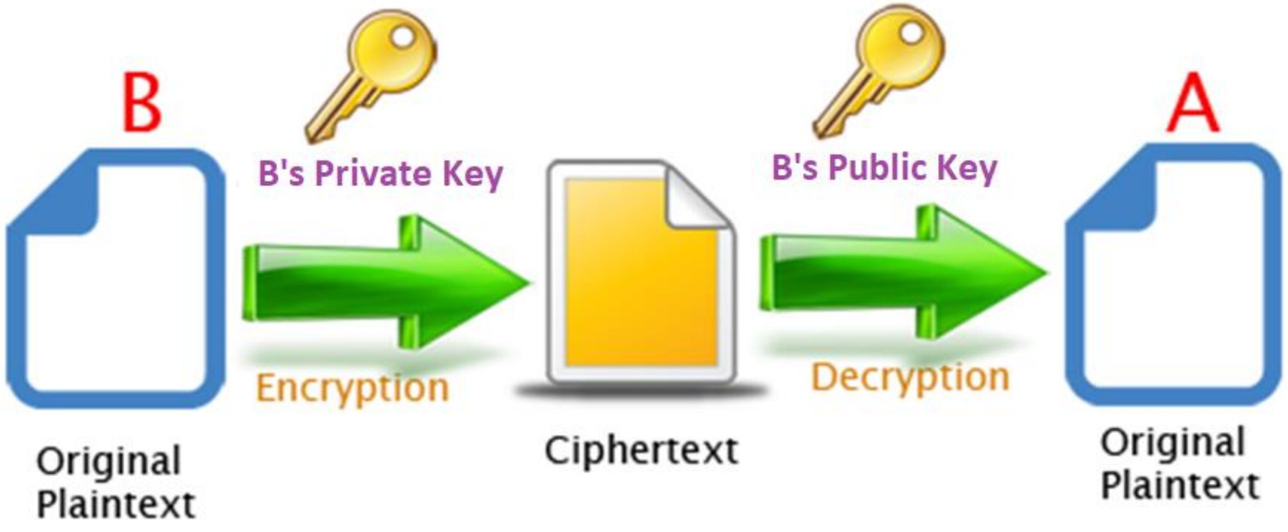
- A digital signature can prove that a message came from a particular sender
- Neither can anyone impersonate the sender nor can the sender deny having sent the message.
- The message is encrypted using the sender's private key. The encrypted message is then sent to the receiver, who can then use the sender's public key to verify the signature.



Digital signatures

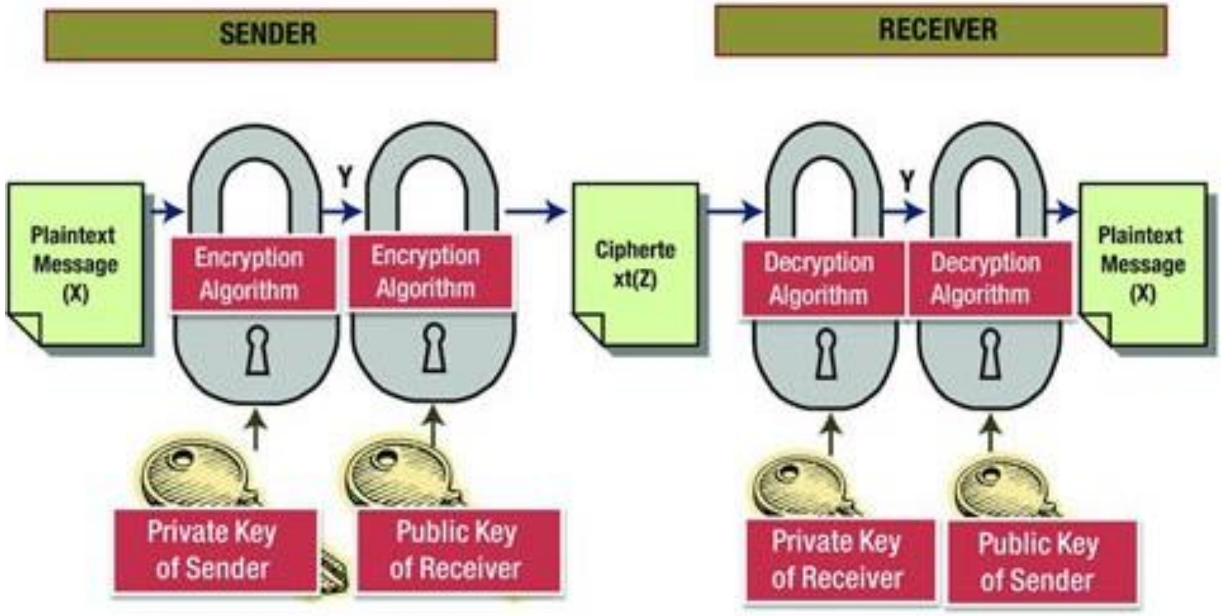
- This is useful for example when making an electronic purchases, allowing the receiver to prove who requested the purchase.

- Digital signatures, however, do not provide confidentiality for the message being sent.



How to Provide secrecy and authentication both?

- For providing secrecy and authentication both, the sender first uses his private Key and then the receiver's public key.



Distribution of Public Keys

- Several techniques have been proposed for the distribution of public keys, which can mostly be grouped into the categories shown.
  - public announcement
  - publicly available directory
  - public-key authority

Public-Key Distribution of Secret Keys

- Once public keys have been distributed using previous methods, secure communication is possible
- However, few users will wish to make exclusive use of public-key encryption for communication because of the relatively slow data rates that can be achieved.
- Accordingly, public-key encryption can be used to distribute the secret keys to be used for conventional/symmetric encryption.
- can also be used for authentication